

Deploying a non-managed SCION AS in the cloud supported by Cyberlink and cloudscale

The SCION production network has seen significant growth in recent years. Notable examples of its deployment include the **Secure Swiss Finance Network (SSFN)** [<https://www.six-group.com/en/products-services/banking-services/ssfn.html>] and the **Secure Swiss Health Network (SSHN)** [<https://support.hin.ch/de/scion/scion-technologie/was-ist-der-hvr-mit-scion/>], both of which support critical infrastructure and are tailored to members of their respective ecosystems.

Recently, our team at **ETH Zurich** received exciting news about SCION's expansion into the cloud. In a joint effort, **cloudscale** [<https://www.cloudscale.ch/>] and **Cyberlink** now offer **native SCION connectivity** to the production network for all customers [<https://www.cyberlink.ch/die-scion-cloud>]. This marks a major milestone: Now, anyone can take advantage of SCION's advanced networking features directly from their servers at cloudscale, without being part of a larger consortium.

Here, we will walk you through the steps we followed to deploy a SCION Autonomous System (AS) in the cloud supported by Cyberlink and cloudscale – exactly as any customer could.

Your very own SCION Cloud – unmanaged

The first step is to get in touch with **cloudscale** and **Cyberlink**, who provided us with detailed information about their SCION offering [<https://www.cyberlink.ch/scion>]. As of the time of writing, they support two types of SCION connectivity:

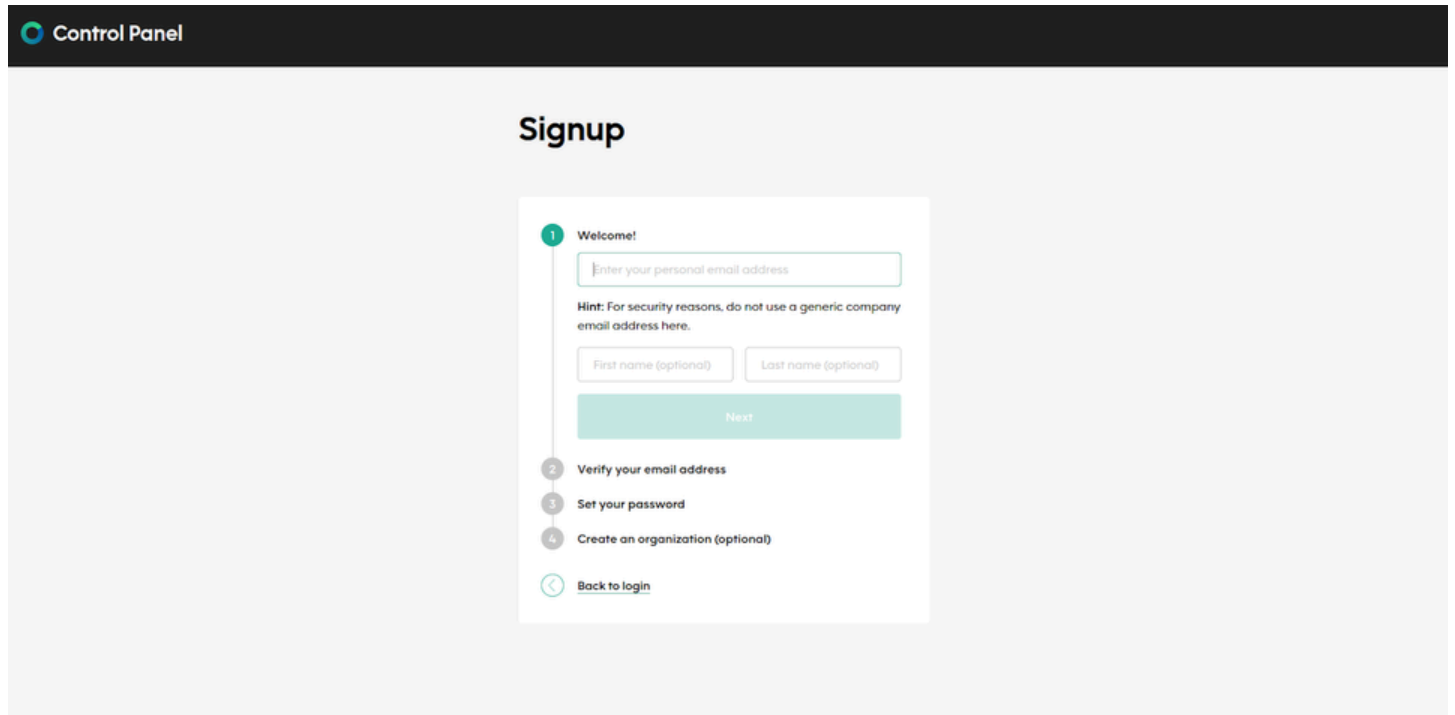
- 1. Non-managed SCION access:** This option provides a direct SCION link to Cyberlink's SCION Border Router at cloudscale within the requested SCION ISolation Domain (ISD). Customers choosing this approach are responsible for deploying and managing their own SCION AS services within their **Virtual Data Center (VDC)**.
- 2. Managed SCION access:** In this setup, Cyberlink handles the deployment and management of SCION services on behalf of the customer, offering a more hands-off experience. The managed access makes use of the Anapaya EDGE appliance.

In this post, we describe the **non-managed** access option, leveraging the **open-source SCION services** [<https://github.com/scionproto/scion>] to set up and operate our own AS. The managed option is described in a

companion article.

Walkthrough

First, we proceeded to create an account and register our organization <https://control.cloudscale.ch/signup>.



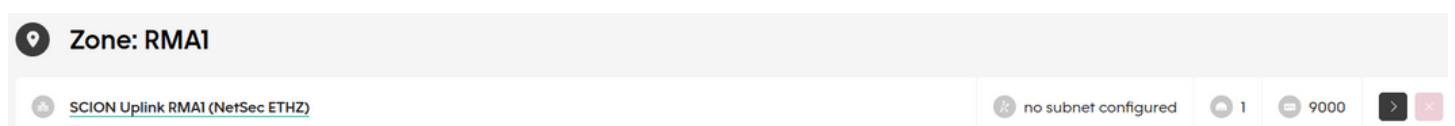
The screenshot shows the 'Control Panel' header in a dark bar. Below it, the 'Signup' section features a multi-step form. Step 1, 'Welcome!', is active and contains an email input field, a hint about using a personal email, optional first and last name fields, and a 'Next' button. Steps 2 through 4 are listed below: 'Verify your email address', 'Set your password', and 'Create an organization (optional)'. A 'Back to login' link is at the bottom left of the form.

We created a **project** within cloudscale to host our SCION-enabled Virtual Data Center (VDC). In parallel, we submitted a request for an **Autonomous System Number (ASN)** to **Anapaya**, the authority responsible for assigning SCION ASNs [<https://docs.anapaya.net/en/release-v0.35/user-guide/certificates/#request-as-number-from-anapaya>]. We provided them with details about our deployment scenario, after which they assigned us an ASN and awaited our **Certificate Signing Request (CSR)**.

Once we had this information, we shared it with Cyberlink. They promptly responded with the necessary configuration details for establishing a **peering session** with their SCION Border Router. These details included:

- cloudscale's ASN within **ISD 64** (the Swiss ISD),
- The **virtual interface** to be used for the network connecting our Border Router to theirs,
- The **IP addresses** for both ends of the link—our Border Router and theirs.

At this point, the new network setup was already visible in our **cloudscale management console**, allowing us to proceed with the configuration.



The screenshot shows a 'Zone: RMA1' header. Below it, a table displays network configuration details. The first row shows 'SCION Uplink RMA1 (NetSec ETHZ)' with a status of 'no subnet configured', a value of '1', and a value of '9000'. There are also expand/collapse and delete icons for each row.

Zone: RMA1					
SCION Uplink RMA1 (NetSec ETHZ)	no subnet configured	1	9000	>	<

With the peering details in place, we proceeded to install and configure the necessary **SCION infrastructure services**. To do this, we deployed a **virtual machine (VM)** within our cloudscale VDC. For our setup, we selected the **Flex 8-4** instance type, running **Ubuntu 22.04 LTS**—a recommended operating system for SCION deployments (Ubuntu 22.04 LTS or newer is advised by the SCION implementation guidelines).

Shared vCPUs

Dedicated CPU Cores

Dedicated GPUs

Flex-4-2

4 GBMemory

2vCPUs

1.65 CHFper day

Change vCPUs

Flex-8-4

8 GBMemory

4vCPUs

3.30 CHFper day

Change vCPUs

Flex-12-6

12 GBMemory

6vCPUs

4.95 CHFper day

Change vCPUs

Flex-16-8

16 GBMemory

8vCPUs

6.60 CHFper day

Change vCPUs

Flex-24-12

24 GBMemory

12vCPUs

9.90 CHFper day

Change vCPUs

Flex-32-16

32 GBMemory

16vCPUs

13.20 CHFper day

Change vCPUs

Flex-48-24

48 GBMemory

24vCPUs

19.80 CHFper day

Change vCPUs

Flex-64-32

64 GBMemory

32vCPUs

26.40 CHFper day

Change vCPUs

Flex-96-48

96 GBMemory

48vCPUs

39.60 CHFper day

Change vCPUs

Flex-128-64

128 GBMemory

64vCPUs

52.80 CHFper day

Change vCPUs

Flex-160-80

160 GBMemory

80vCPUs

66.00 CHFper day

Change vCPUs

Flex-192-96

192 GBMemory

96vCPUs

79.20 CHFper day

Change vCPUs

As mentioned earlier, we installed the **open-source SCION software**. To streamline the deployment process, we used the recently developed **SCION Orchestrator** [<https://github.com/scionproto-contrib/scion-orchestrator>], a tool designed to simplify the installation, configuration, and management of SCION services.

We downloaded the latest release bundle and ran the **scion-orchestrator** installer. This binary sets up the core SCION services and guides the user to access the **web-based interface** via <https://localhost:8843>. Upon first access, the interface launches an **installation wizard** that walks the user through the initial configuration steps.

Install Wizard

Follow the steps to complete your setup



Welcome

2

General

3

Configuration

4

Account

5

Install

Configure your Node here

ISD-AS

Install Directory

Back

Next

After completing the initial configuration, we reloaded the GUI as instructed. Upon entering our credentials, we gained access to the **admin console**, which serves as the central interface for managing the SCION Autonomous System (AS). From this console, administrators can configure key aspects of the SCION AS, including service parameters, certificates, and peering relationships.

Welcome to Scion Orchestrator

A powerful tool to manage your SCION Autonomous System.

First Steps

- 1) Generate a Certificate Signing Request and send it to your CA.
- 2) Upload your certificate chain once received from your CA.
- 3) Add your first SCION link to get upstream connectivity.

Need Help?

Follow the steps above to configure your SCION AS and ensure it's up and running. If you need assistance, visit our [documentation](#) or reach out to support.

The next key step is to generate a **Certificate Signing Request (CSR)**. Using the admin console, we filled in the required fields as specified in the official SCION documentation. Once completed, the system generated a `.csr` file, which we would later submit to the SCION authority for signing (in this case Anapaya).

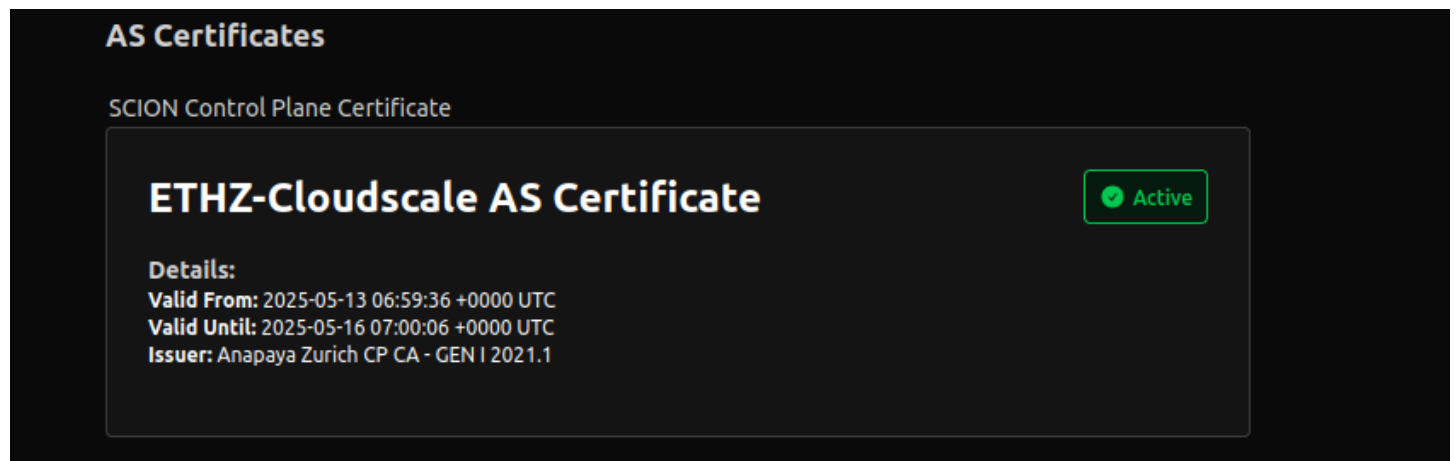
The screenshot displays the SCION Orchestrator web interface. On the left is a navigation sidebar with links for Home, Cryptography (selected), Troubleshooting, and Connectivity. The main content area is titled 'Certificate Signing Requests' under the 'Cryptography' navigation. It features a 'Generate Certificate Signing Request' form with a text area containing a JSON object:

```
{  "subject": {    "common_name": "1-150 AS Certificate",    "id_as": "1-150"  }}
```

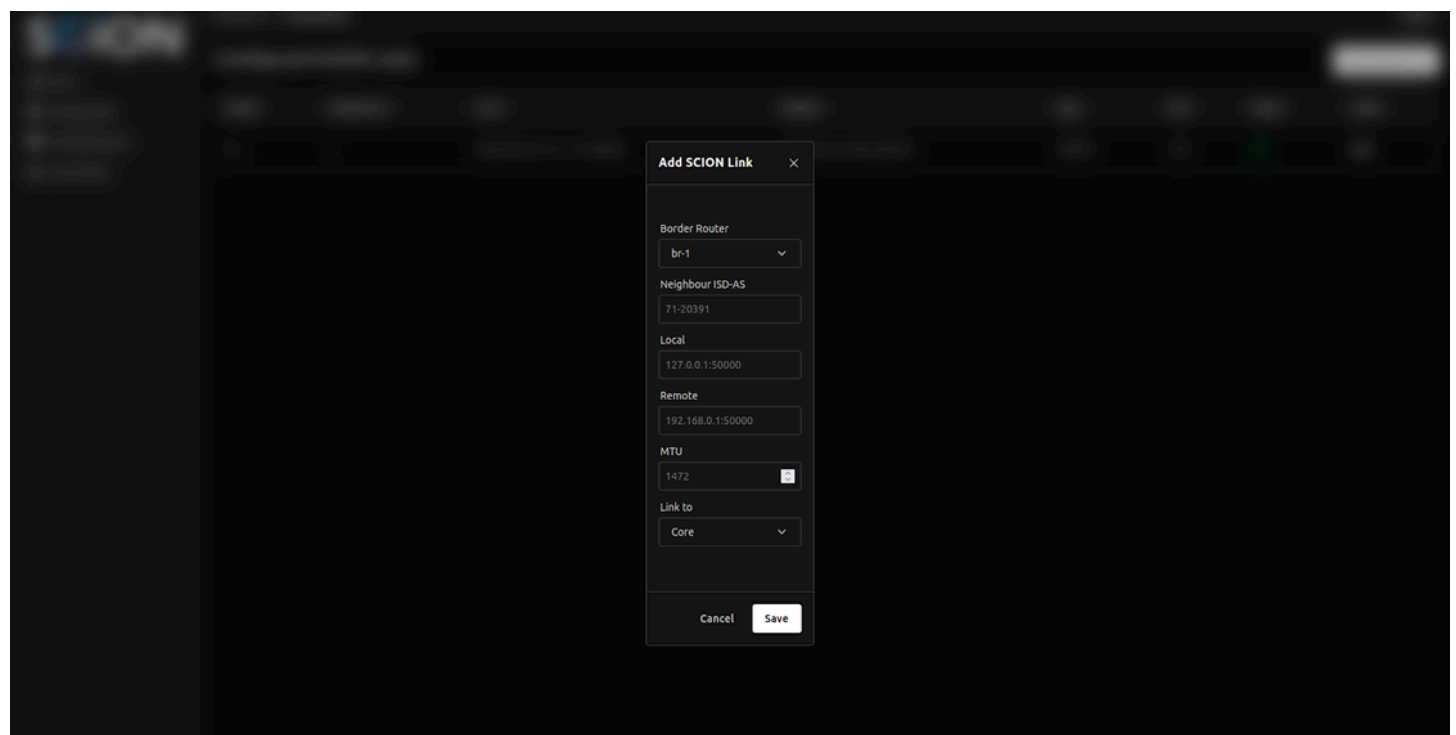
. Below the form is a 'Generate' button. Underneath, a 'Result' section contains a large empty text area for the output, with 'Copy CSR To Clipboard' and 'Download CSR' buttons at the bottom. To the right, the 'AS Certificates' section shows 'No Certificate Found' for the 'SCION Control Plane Certificate' and includes a 'No Certificate Available' error message. Below this, the 'Upload new Certificate Chains' section has a 'Choose Certificate Chain' dropdown, a 'Browse...' button (showing 'No file selected'), and an 'Upload Certificate Chain' button.

In addition to the CSR, this process also creates the necessary **cryptographic material** locally, including the private key, required for secure SCION AS operation.

We submitted the `.csr` file to **Anapaya**, and within a few minutes, they returned our signed **SCION certificate**. Using the admin console, we uploaded the certificate to complete the trust setup.



Next, we configured the **SCION peering session** with cloudscale's Border Router. To do this, we navigated to the **"Connectivity"** section in the admin console and selected **"Add SCION link."** We filled in the required fields using the configuration details previously provided by Cyberlink and saved the setup. If everything is configured correctly, the link status appears as **"Active."**



With the link established, our SCION AS was fully operational. We verified connectivity by checking whether we could **fetch paths to other ASes** in the SCION production network.

```

@ :~$ scion showpaths 64-2:0:9 -m 20
Available paths to 64-2:0:9
4 Hops:
[ 0] Hops: [64-2:0:9c 1>36 64-59414 5>34 64-559 5>1 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[ 1] Hops: [64-2:0:9c 1>36 64-59414 5>34 64-559 6>2 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[ 2] Hops: [64-2:0:9c 1>36 64-59414 6>33 64-559 5>1 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[ 3] Hops: [64-2:0:9c 1>36 64-59414 6>33 64-559 6>2 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
5 Hops:
[ 4] Hops: [64-2:0:9c 1>36 64-59414 1>23 64-15623 8>21 64-559 5>1 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[ 5] Hops: [64-2:0:9c 1>36 64-59414 1>23 64-15623 8>21 64-559 6>2 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[ 6] Hops: [64-2:0:9c 1>36 64-59414 1>23 64-15623 9>22 64-559 5>1 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[ 7] Hops: [64-2:0:9c 1>36 64-59414 1>23 64-15623 9>22 64-559 6>2 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[ 8] Hops: [64-2:0:9c 1>36 64-59414 4>34 64-6730 9>15 64-559 5>1 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[ 9] Hops: [64-2:0:9c 1>36 64-59414 4>34 64-6730 9>15 64-559 6>2 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[10] Hops: [64-2:0:9c 1>36 64-59414 4>34 64-6730 10>16 64-559 5>1 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[11] Hops: [64-2:0:9c 1>36 64-59414 4>34 64-6730 10>16 64-559 6>2 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[12] Hops: [64-2:0:9c 1>36 64-59414 7>34 64-2:0:13 16>20 64-559 5>1 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[13] Hops: [64-2:0:9c 1>36 64-59414 7>34 64-2:0:13 16>20 64-559 6>2 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[14] Hops: [64-2:0:9c 1>36 64-59414 7>34 64-2:0:13 31>31 64-559 5>1 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[15] Hops: [64-2:0:9c 1>36 64-59414 7>34 64-2:0:13 31>31 64-559 6>2 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[16] Hops: [64-2:0:9c 1>36 64-59414 9>35 64-6730 9>15 64-559 5>1 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[17] Hops: [64-2:0:9c 1>36 64-59414 9>35 64-6730 9>15 64-559 6>2 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[18] Hops: [64-2:0:9c 1>36 64-59414 9>35 64-6730 10>16 64-559 5>1 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:
[19] Hops: [64-2:0:9c 1>36 64-59414 9>35 64-6730 10>16 64-559 6>2 64-2:0:9] MTU: 1452 NextHop: Status: alive LocalIP:

```

Additionally, the orchestrator service will take care of renewing the SCION certificates in the background so that our SCION connectivity is not interrupted by certificate expirations.

Setting up a SCION AS within cloudscale's infrastructure proved to be a smooth and well-supported process, thanks to the combination of the native SCION connectivity provided by Cyberlink and cloudscale and the tooling provided by the SCION open-source ecosystem. With the help of the **SCION Orchestrator**, we were able to deploy, configure, and bring our AS online with minimal friction. The ability to independently manage our SCION services while benefiting from cloudscale's production-grade connectivity opens up exciting possibilities for research, development, and real-world applications. This setup not only demonstrates the SCION-cloud integration but also lowers the barrier for broader adoption across diverse ecosystems.

Once configured, this access offers instant high-availability connectivity to any entity in the SCION ecosystem, similar to a leased line. Although the SCION setup effort requires about 1 hour, secure connectivity can now be established within milliseconds!

Remember to check out our companion post for the **Managed SCION access** setup.

Congrats to cloudscale and Cyberlink for this exciting offering!

About cloudscale:

cloudscale is a leading technology company specializing in cloud infrastructure, with a strong focus on security, performance and scalability. With data centers in Switzerland and ISO 27001 certification, cloudscale supports its customers in meeting compliance requirements.

About Cyberlink:

Cyberlink is a Swiss managed service provider based in Zürich that specializes in the development and provision of state-of-the-art IT solutions. Cyberlink's core competencies are innovative cloud solutions, site interconnection and customized business Internet solutions.

